QR codes, "Quick Response Codes," are all around us. These square, black and white boxes allow businesses to quickly direct you to their web site, can track product information in a supply chain, link us to applications as well as store financial information. The uses for these codes are nearly limitless as they store a great deal of data in a very small space.
Our smartphones scan the pattern simply by pointing the phone's camera at the code.

As is often the case, criminals and scammers find methods to steal personal data and money using these very same technologies.

Nationwide, law enforcement agencies are receiving numerous calls regarding altered QR codes designed to illegally obtain a victim's banking information, credit card information and/or personal data stored on their smartphone.

Scammers are always searching for ways to separate you from your money and they have discovered that the use of fraudulent QR codes is an effective way to do so.

For example, QR code scams involving parking fees have been reported across the nation. "Scan to pay" stickers are placed on parking meters and around public parking locations. Most of us are in a hurry to get to our destination and pay little attention to where our parking fees are being sent.

Many reports have been received regarding fraudulent discount coupons being sent via email or text messaging. By copying a legitimate ad from a reputable retailer, scammers then cut and paste their QR code over the legitimate one. By doing so, you are redirected to a phishing website capable of stealing credit card and personal information.

Please consider the following methods of prevention:

Do not scan a randomly found QR code. Be selective!

Look for QR code tampering such a sticker placed over an existing QR code. Some scammers are physically pasting bogus codes over legitimate ones. If it looks as though a code has been tampered with at your local bar or restaurant, don't use it. This applies to legitimate ads you obtain or receive in the mail.

Be suspicious if, after scanning a QR code, the site asks for a password or login info.

Do not scan QR codes received in emails unless you know they are legitimate. Call the sender to confirm.

Carefully review the destination page.

Should you be victimized by a fraudulent QR code, please contact the FBI's Internet Crime Complaint Center at www.ic3.gov or call your FBI local office. Fraud can also be reported to the Federal Trade Commission by visiting ReportFraud.ftc.gov.